WPI Acc No: 98-558382/199848
XRPX Acc No: N98-435346
Mutual authentication method of communicating units - generating random number by first unit which encrypts random numbers generated by first and second units and secrete key only known by first unit with secrete key known by both units for transmission and decryption by second unit
Patent Assignee: GIESECKE & DEVRIENT GMBH (GIES-N)
Inventor: FROHLICH H; GALL W; FROEHLICH H; GAAL W
Number of Countries: 082 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 19716111	A1	19981022	DE 1016111	A	19970417	H04L-009/32	199848 B
WO 9848389	A2	19981029	WO 98EP2231	A	19980416	G07F-007/10	199849
AU 9880135	A	19981113	AU 9880135	A	19980416	G07F-007/10	199913

Priority Applications (No Type Date): DE 1016111 A 19970417
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
DE 19716111	A1		4			
WO 9848389	A2	G				

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9880135	A		Based on			WO 9848389

Abstract (Basic): DE 19716111 A

The method involves generating a random number by a second unit (B) which is transmitted to first unit (A) which selects a secret key (Ks) only known by the first unit. The first unit encrypts a random number (Za) generated by the first unit using a secrete key (Kab) known by both units. The random number generated by the second unit and the selected secrete key are encrypted as well by the first unit. The result is transmitted as a message (N1) to the second unit which decrypts the received message using the mutual secrete key.

The second unit compares the random number generated by the second unit with the number obtained by decrypting the random number received by the first unit. When the numbers are in conformance the first unit is authenticated by the second unit. The second unit encrypts with the received and decrypted key of the first unit the *random* *number* *generated* by the first unit and transmits the result. The first unit decrypts the received message and compares the generated random number with the number received from the second unit. When the numbers are in conformance the second unit is authenticated by the first unit.

USE - E.g. for chipcard and terminal, mobile radio system.

ADVANTAGE - Prevents appearance of plain text and key during communication and increases security. Enables key exchange during authentication without administration. Allows key to be dynamic and different for each authentication.

Dwg.1/1

Title Terms: MUTUAL; AUTHENTICITY; METHOD; COMMUNICATE; UNIT; GENERATE; RANDOM; NUMBER; FIRST; UNIT; RANDOM; NUMBER; GENERATE; FIRST; SECOND; UNIT; SECRETION; KEY; FIRST; UNIT; SECRETION; KEY; UNIT; TRANSMISSION; DECRYPTER; SECOND; UNIT